DETAILED ACTION

1. This action is responsive to communications: application, filed 12/29/2003; amendment filed 12/28/2009.

2. The text of all prior office actions are hereby incorporated by reference.

3. Claims 42-50 and 52-78 are pending. Claim 51 is cancelled.

Response to Arguments

4. Applicant has cancelled claim 51. Accordingly, the rejection under section 112 associated with claim 51 is withdrawn. Applicant's argument relative to prior art rejection against pending claims has been considered, but is not persuasive as discussed in detail in the following.

Applicant argues: "The applied art is not understood to disclose or to suggest the foregoing features of claim 1. In particular, the cited references do not disclose or suggest that each buffer element has a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores (emphasis added)."

As indicated in the rejection, Ohta paragraph [0011] teaches "a data block accumulation unit that outputs the accumulated amount to the authentication processing unit when it reaches the smallest data block size for the authenticating processing". This teaches that the buffer size to store accumulated amount should be at least as large as the smallest data block size for the authentication processing. In other words, the logic of Ohta's system considers enough buffer size to accommodate the data blocks, and this consideration is also based on the blocks sizes for each authentication algorithm. Since the accumulated data is output to the buffers as soon as it reaches the smallest data block size for processing, there would be no authentication block size larger than that smallest block size.

More importantly, the rejection states that it is only logical for the one skilled in art to consider enough buffer sizes to accommodate data blocks. The one skilled in art knows that if there is not enough buffer size, the computer process will crash. Given that Ohta teaches that the block size of the authentication algorithm must be considered (see above), it would be obvious to have buffers at least as large as the largest block size. With regards to this argument, applicant argues that Ohta does not teach different authentication algorithms. However, first Ohta does teach the block size of an authentication algorithm must be considered. Second, the rejection is based on a combination that teaches different authentication algorithms, with different sizes. Therefore, the combination of cited prior arts does teach different algorithms with different sizes, and applicant's arguments non-persuasive.

With respect to claims 58, 68, 44, 53, 65 and 77 applicant argues that that the feature one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks is not taught by the cited prior art. Applicant argues that examiner's statement that Ohta paragraph [0016] teaches outputting blocks of data to the encryption and authentication processors in multiples of 8 bits is incorrect. However, as admitted by the applicant, paragraph [0016] teaches that the data block for encryption processing **can be** 64 bits, which is clearly a multiple of 8 bits (one byte). The claim requirement is 16 bytes and 64 bytes, which are clearly multiples of one byte. In addition, the example cited in paragraph [0016] teaches the option of processing different data block sizes. This makes it obvious to process a specific data block size (such as 16-bye or 64-byte), unless there is an unexpected result associated with those specific numbers. In other words, barring any unexpected results, the size of a data block (16-byte or 64-byte) is an obvious design choice. Applicant's specification or argument does not discuss any unexpected result or specific advantage in selecting those specific numbers. Therefore, said requirement is made obvious by the cited prior art, as it teaches options in different data block sizes.

With respect to claims 52, 68, 48, 60, 66 and 78 applicant makes the similar argument as discussed above regarding claims 58, 68, 44, 53, 65 and 77. For the same reasons discussed above, the argument is non-persuasive. Applicant also argues that Ohta does not teach two cipher cores because Ohta only teaches a single cipher core. However, as indicated in the rejection, Ohta Figure 12 and associated text show a plurality of cipher cores (303a and 303b). Applicant does not discuss the cited portion of Ohta, and therefore the argument is no more than a mere general allegation.

Accordingly, applicant's arguments are found non-persuasive, and all prior art rejections are maintained.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 42, 44-45, 48-50, 52, 53, 55-56, 58, 60, 62, 63, 65-70, 72-77 are rejected under 35 U SC. 103(a) as being unpatentable over Ohta et al. (US 2002/0083317) hereinafter called Ohta, in view of Tardo (US 7,082,534)

6.1. Claim 42 disclose a processor, comprising: a crypto unit configured to process processing contexts, each processing context configured to process a respective data packet at a time and to store cipher keys and algorithm context associated with processing the data packet (Ohta Paragraph [0012] teaches plural cipher processing units and paragraph [0046] teaches different cipher algorithms used to encrypt/decrypt the data. This would correspond to the "plurality of processing contexts"), each processing context comprising authentication of the at least one packet (paragraph [0046] and [0011] show that when a packet requires authentication and/or encryption, it will be routed to an authentication processing unit and/or encryption processing unit. Therefore, when a packet requires authentication, it will be assigned a processing context to perform authentication. Naturally, performing cipher operations requires storing the cipher key and associated algorithm);

the crypto unit comprising:

a cipher core configured to cipher data received; (Ohta Figure 12 and associated text show a plurality of cipher cores (303a and 303b) and a plurality of authentication buffers (304a and 304b))

Ohta teaches authentication cores configured to authenticate the ciphered data in Figure 12, Authentication Processing Unit 305a and 305b and associated text in paragraph [0104]. Ohta also teaches authentication buffers (Data Block Accumulation Unit) connected to authentication cores as shown in figures 2, 3, 10, 12, 13, 16, or 18 and their associated text. Ohta does not teach but Tardo teaches, at least two authentications cores each implementing a different authentication algorithm as shown in Figures 2 and 3 and explained in column 4 lines 48-67 through column 5 lines 1-36. Figure 2 shows 2 authentication engines MD5 225 and SHA1 227. Figure 3 and associated text teach choosing the authentication engine based on the encryption as in column 5 lines 25-29. It would be obvious to one of ordinary skill in the art at the time of invention to use 2 different authentication algorithms of Tardo in two different authentication cores of Ohta. The motivation to combine would be that in paragraph [0046] of Ohta it states that the authentication algorithm includes HMAC-MD5-96 and HMAC-SHA-1-96. Therefore, as shown in Ohta the authentication cores include different algorithms) and requiring a different authentication algorithm block size (Tardo col. 7 lines 20-40. Also Tardo col. 4, lines 1-14 suggests using authentication and ciphering protocols, such as MD4, MD5, etc. which require different block sizes. Tardo also refers to the text book Applied Cryptography, for different authentication and encryption algorithms. The book provides many examples of authentication algorithms with different block sizes); and

an authentication buffer connected to the cipher core (see above or Ohta figures 2 or 12 and associated text) comprising buffer elements, each buffer element storing data corresponding to a respective one of the processing contexts (Figure 12 shows two buffers and two authentication processing units. Note also that as stated before, each packet requiring authentication will be stored (buffered) in a data accumulation unit until it is ready for encryption), and having a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores, the authentication buffer configured to store the ciphered data and provide the ciphered data to the authentication cores each in an amount based on the corresponding authentication algorithm implemented. (Ohta Figure 12, Data Accumulation Unit 304a and 304b; paragraph [0011] states "a data block accumulation unit that outputs the accumulated amount to the authentication processing unit when it reaches the smallest data block size for the authentication processing". Note further that Ohta teaches breaking a packet to smaller fragments and processing each fragment based on an encryption or authentication algorithm (see figures 1 and 2 and associated text), and storing fragments in buffers before they are ready for processing. It would be only logical to have a buffer size that is large enough to accommodate the largest block size (fragment)).

6.2. Claim 44 discloses the processor according to claim 42, wherein one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks. (The rejection of claim one above and also, Ohta paragraph [0016] teaches outputting blocks of data to the encryption and authentication processors in multiples of 8 bits, which would include all processor blocks in claims 44 and 45.)

6.3. Claim 45 discloses the network processor according to claim 42, wherein crypto unit further comprises cipher cores configured to cipher data and authentication buffer comprises authentication buffer elements (Ohta figure 12 shows multiple encryption processing units and multiple data block accumulation units).

6.6. Claim 48 discloses the network processor according to claim 45, wherein one of the cipher core cores processes data in 8-byte blocks and another one of the cipher cores processes data in and/or 16-byte blocks. (The rejection of claim one above and also, Ohta paragraph [0016] teaches outputting blocks of data to the encryption and authentication processors in multiples of 8 bits, which would include all processor blocks in claims 44 and 45.)

6.7. Claim 49 discloses processor of claim 45 wherein the number of processing contexts does not equal a number of the cipher cores (processing contexts are comprised of a combination of authentication processing and/or encryption processes with the associated buffers, as shown in Ohta paragraph [0042]. Therefore, the system assigns a processing context for a packet, which may or may not require authentication. Therefore, the number of processing contexts is not equal to the number of authentication cores when a packet only requires encryption. Note also that as mentioned above, and according to Tardo's teachings, the system of Ohta in view of Tardo may include several authentication cores, each corresponding to a different authentication protocol, and therefore, the number of authentication cores may not be equal to number of processing contexts. Ohta in view of Tardo teach the number of cipher cores unequal to the number of processing contexts the same way as it teaches the number of authentication cores unequal to processing contexts).

6.8. Claim 50 discloses the processor of claim 49 wherein the number of the plurality of processing contexts is six, a number of the buffer elements is six, the number of the plurality of cipher cores is four and the number of the authentication cores is five (Ohta in view of Tardo teaches a system with a plurality of buffers, each corresponding to each processing context and a flexible number of authentication and cipher cores (not necessarily equal to the number of processing contexts, as discussed in claims 1 and 36). Therefore, barring any unexpected results, it would have been obvious to the one skilled in art to have six processing contexts, with a buffer each, and four cipher cores, and five authentication cores. Note that the examples shown in the applicant's specification are just example scenarios, and no special feature or advantage is named with regards to those specific numbers for buffers, processing context, cipher cores, or authentication cores).

6.9. Claim 51 is cancelled.

6.10. As per claim 52, the requirements are substantially the same as claims 42-51 above. Note that Ohta figure 12 shows connection pathways connecting different elements, and therefore teaches a first and second bus connecting the elements.

6.11. As per claim 62, Ohta paragraph 89 teaches a configuration that the device is also a router.

6.12. As per claims 73, 74 and 75, Ohta in view of Tardo teaches ciphering data received in a first cipher core and using a first algorithm, because as shown in rejection of claim 42, the system includes ciphering cores and performs ciphering and authentication using multiple algorithms.

6.13. As per claim 76, Ohta paragraph 8 teaches parallel processing of packets.

6.14. As per claims 53, 55-56, 58, 60, 63, 65-70, 72, 77-78, the requirements are substantially the same as claims 42, 44-45, 48-52, 62, 73-76 above.

7. Claims 46, 47, 54 and 61are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohta et al. (US 200210083317) in view of Tardo (US 7,082,534), and further in view of Corder (US 7,069,447).

7.1. As per claims 46 and 47, Ohta and Tardo teach claim 45. However, Ohta in view of Tardo does not teach a connection using a multiplexer device. Ohta teaches connections using a data path connection switching unit as in paragraph [0013].

Corder teaches authentication and encryption buffers and units connected with a multiplexer in column 7 lines 1-21.

Ohta in view of Tardo and Corder are analogous art, as they are directed to security systems performing encryption and authentication comprising processors and buffers connected via data paths. At the time of invention, it would have been obvious to use multiplexer devices as connection paths for connecting authentication and encryption buffers as taught by Corder to connect processors and buffers in Ohta in view of Tardo. The motivation to do so is providing various, flexible connection paths between elements, as suggested by Ohta paragraph [0129] , where it teaches that the data path connection switching unit is used to provide various paths flexibly combined to fully take advantage of the multiple units. Therefore it would be obvious to one of ordinary skill in the art at the time of invention that this same inherent property of a multiplexer would be an alternate choice.

7.2. As per claims 54 and 61, the requirements are substantially the same as claims 46 and 47 above.

8. Claims 43, 57, 59, 64, and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohta et al. (US 2002/0083317) and Tardo (US 7,082,534), and further in view of “Speculation Techniques for Improving Load Related Instruction Scheduling”, published in 1999, herein referred to as Spe.

8.1. Claim 43 discloses the processor according to claim 42.

Ohta in view of Tardo does not teach processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the plurality of processing contexts with processing of the packet data in a second portion of the plurality of processing contexts.

Spe teaches processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the plurality of processing contexts with processing of the packet data in a second portion of the plurality of processing contexts (Spe section 2.3 shows how downloading different portions of an execution program (packet data and key info as one portion, and processing of packet data as the other portion) into different pipelined banks hides the execution latency).

It would be obvious to one of ordinary skill in the art at the time of invention was made to use pipelining to hide the latency of data within the system of Ohta in view of Tardo, since Spe states at sections 1 and 2.3 that its method minimizes the stall time caused by waiting for missing data, for example the authentication buffer in Ohta.

8.2. As per claims 57, 59, 64, and 71 the requirements are substantially the same as claim 43 above.

Conclusion

9. **THIS ACTION IS MADE FINAL**. See MPEP § 7.39. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7874. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Farid Homayounmehr/

Examiner,

AU:2439

4/7/2009